UNITED STATES BANKRUPTCY COURT
SOUTHERN DISTRICT OF NEW YORK

In re: CELSIUS NETWORK LLC, *et al.,* Post-Effective Date Debtors.	**NOT FOR PUBLICATION** Case No. 22-10964 (MG) Chapter 11
MOHSIN Y. MEGHJI, as Representative for the Post-Effective Date Debtors, Plaintiff, v. CHRISTOPHER SPADAFORA and CLOUDFLARE, INC., Defendants.	Adv. Pro. No. 24-03981 (MG)

MEMORANDUM OPINION AND ORDER DENYING CLOUDFLARE MOTION TO DISMISS

APPEARANCES:

MAYER BROWN LLP
Attorneys for Defendant Cloudflare, Inc.
1221 Avenue of the Americas
New York, New York 10020
By: Matthew D. Ingber, Esq.
Niketa K. Patel, Esq.
Joaquin M. C de Baca, Esq.
David Yolkut, Esq.

WHITE & CASE LLP
Attorneys for Representative of Post-Effective Date Debtors
1221 Avenue of the Americas
New York, NY 10020
By: Joshua D. Weedman, Esq.
Samuel P. Hershey, Esq.
Renza Demoulin, Esq.

MARTIN GLENN
CHIEF UNITED STATES BANKRUPTCY JUDGE

Pending before the Court is the motion to dismiss (the "Motion," ECF Doc. # 7) of Cloudflare, Inc. ("Cloudflare" or the "Defendant") seeking entry of an order dismissing all claims asserted against it in the Complaint (the "Complaint," ECF Doc. #1) filed by Mohsin Meghji ("Litigation Administrator" or the "Plaintiff"), in his capacity as Litigation Administrator of the estates of the above-captioned debtors and debtors-in-possession (collectively, the "Debtors," and together with their non-Debtor affiliates "Celsius" or the "Company") appointed pursuant to the Modified Joint Chapter 11 Plan of Reorganization of Celsius Network LLC and its Debtor Affiliates (the "Plan"). Annexed to the Motion are (i) a proposed order granting the Motion as Exhibit A; and (ii) a memorandum of law in support of the Motion (ECF Doc. # 8). The Plaintiff filed a memorandum of law in opposition to the Motion (the "Opposition," ECF Doc. # 16). Cloudflare filed a memorandum of law in further support of the Motion (the "Reply," ECF Doc. # 21).

For the reasons discussed below, the Court: **DENIES** Cloudflare's Motion to Dismiss.[1]

I. BACKGROUND

A. The Complaint

The Complaint asserts two causes of actions against Defendant Cloudflare, Inc.: (i) negligence and (ii) gross negligence, both arising from an alleged failure to maintain adequate cybersecurity protections related to the issuance and management of API keys for the BadgerDAO platform. (Complaint ¶ 80-94.)

[1] The Court already entered a Memorandum Opinion and Order Denying the motion to dismiss of co-defendant Christopher Spadafora. *See Meghji v. Spadafora,* 2025 WL 1232578 (MG)(Bankr. S.D.N.Y. April 28, 2025).

1. First Cause of Action: Negligence

Celsius first alleges that Cloudflare's conduct constituted negligence. Celsius alleges that Cloudflare owed a duty to BadgerDAO and all its governing members, including Celsius, to implement adequate security protocols for the issuance of API keys granting access to BadgerDAO's API. (*Id*. ¶ 81.) This duty allegedly arose from Cloudflare's agreement to secure access to accounts containing sensitive passphrases like API keys. (*Id*. ¶ 82.)

There was a flaw in Cloudflare's system that initially went unnoticed but was eventually fixed. (*Id*. ¶ 84.) Celsius claims that all BadgerDAO members, including Celsius, reasonably expected Cloudflare to warn users if a vulnerability may have compromised their sensitive information prior to the flaw being remedied. (*Id*.) However, Cloudflare did not issue such a warning. (*Id*.) Accordingly, Celsius claims that Cloudflare breached its duty to BadgerDAO and Celsius by issuing API keys prior to proper account verification and by failing to notify users of the vulnerability after it was discovered. (*Id*. ¶ 85.)

Celsius further alleges that this breach was the proximate and but-for cause of Celsius' injury. (*Id*. ¶ 86.) Specifically, the Complaint asserts that a hacker was able to gain unauthorized access to BadgerDAO's systems by obtaining an API key in mid-September and remained undetected for over two months, ultimately executing a first fraudulent transfer of funds on November 20, 2021. (*Id*.)

As a result, Celsius asserts that Cloudflare's failure to exercise the degree of care required by industry standards and by a reasonably prudent person under similar circumstances constitutes negligence and caused Celsius to lose more than $50 million in assets stored on the BadgerDAO platform. (*Id*. ¶ 87-88.)

2. Second Cause of Action: Gross Negligence

Celsius further alleges in the second cause of action that Cloudflare's conduct constituted gross negligence. The Complaint asserts that Cloudflare breached its duty to Celsius when it failed to remedy the known vulnerability in its systems, which created an unreasonable risk of harm to all users of BadgerDAO, including Celsius. (*Id*. ¶ 92.) Specifically, Cloudflare had been informed of this vulnerability and was aware that it allowed malicious actors to potentially access the developer-end or API of its clients' platforms—many of which, like BadgerDAO, were used to safeguard significant sums of customer funds. (*Id*.) By failing to immediately remedy the vulnerability, and by subsequently failing to notify users that their APIs, and therefore their funds, might have been compromised, Cloudflare created an unreasonable risk of harm to its users, including BadgerDAO, and in turn, to BadgerDAO's users, including Celsius. (*Id*.) Cloudflare's failure to act was therefore grossly negligent. (*Id*. ¶ 93.)

As a result of Cloudflare's alleged breach and its failure to exercise even slight care or diligence in fixing a known issue that had been reported on multiple occasions or notifying BadgerDAO of a vulnerability, Celsius claims it has suffered damages, amounting to over $50 million in assets, following the hack of the BadgerDAO platform. (*Id*. ¶ 94.)

B. The Cloudflare's Motion to Dismiss

Cloudflare filed the Motion to dismiss all claims asserted against it in the Complaint. (Motion at 1-2.) Cloudflare argues that Celsius fails to state both a negligence claim and a gross negligence claim. (*Id*.)

Cloudflare argues that it owes no legal duty to Celsius, as there was no direct relationship, contract, or special connection between them. (ECF Doc. #8 at 16-21.) This absence of relationship, Cloudflare alleges, is fatal to the negligence claim. (*Id*. at 16.)

Cloudflare claims that New York law recognizes an exception to the general rule that there is no duty to protect others from injuries caused by third parties if there is a special relationship exists, either between either between defendant and a third-person tortfeasor that encompasses defendant's actual control of the third person's actions, or between defendant and plaintiff that requires defendant to protect plaintiff from the conduct of others. (*Id*. at 20.) Cloudflare claims Celsius failed to allege either form of special relationship as Cloudflare had no contacts or dealings either with the criminal hackers or with Celsius. (*Id*.)

Furthermore, Cloudflare claims Celsius failed to allege any breach by Cloudflare because it has failed to plausibly allege that Cloudflare owed it any duty of care. (*Id*. at 23.) Celsius' negligence claim fails for the additional and independent reason, Cloudflare argues, that Plaintiff's allegations on causation are "reed-thin," and that certain actions by BadgerDAO, third-party hackers, or Celsius are intervening causes to Cloudflare's breach. (*Id*. at 24-25.)

Cloudflare further contends that Celsius' gross negligence claim fails for the same reasons as its ordinary negligence claim, and additionally lacks the heightened culpability required under New York law. (*Id*. at 28.) Gross negligence requires conduct that demonstrates reckless disregard or intentional wrongdoing, far beyond ordinary carelessness. (*Id*. at 29.) Celsius merely alleges that Cloudflare was aware of a potential API key vulnerability discussed in a public forum and failed to act quickly enough. (*Id*.) However, Cloudflare notes it responded within days and addressed the issue, which cannot reasonably be characterized as reckless. (*Id*. at 30.)

C. The Opposition

Celsius filed the Opposition to the Motion. For the negligence claim**,** Celsius argues that Cloudflare owed Celsius a duty of care because of a special relationship formed through

Cloudflare's role in securing access to the BadgerDAO platform. (Opposition ¶ 10.) Celsius argues that it has adequately pleaded proximate cause since Cloudflare's actions breach a clearly established industry standard and there were no intervening causes to Cloudflare's Breach. (*Id*. ¶ 35.)

For the gross negligence claim, the plaintiff claims Cloudflare acted with gross negligence by showing a reckless disregard for the safety of its users. (*Id*. ¶ 39.) Cloudflare allegedly ignored repeated warnings about a security flaw and failed to implement safeguards in a timely manner. (*Id*. ¶ 40.) This indifference, particularly in a high-stakes environment involving large crypto assets, should be characterized as an extreme departure from standard conduct. (*Id*.) Cloudflare's defense—that it responded within two days and intended to fix the issue—raises factual disputes inappropriate for resolution at the motion to dismiss stage. (*Id*. ¶ 41.) Additionally, Cloudflare's claim that it lacked knowledge of the vulnerability is contradicted by its own admission of recognizing increased abnormal activity. (*Id*. ¶ 42.)

D. Cloudflare's Reply

Cloudflare filed the Reply to the Opposition. Cloudflare argues that Celsius fails to state a negligence claim because there was no duty of care owed, as Cloudflare had no direct relationship, control, or interaction with Celsius, and did not handle its data. (Reply at 8-10.) It also challenges Celsius' claim to be a general partner of BadgerDAO, pointing out that Celsius disclaimed any actual control or governance. (*Id*. at 12.) Cloudflare argues that even if it had been negligent, BadgerDAO's failure to implement basic security and reliance on a free service without adequate safeguards were unforeseeable intervening acts that break the chain of proximate causation. (*Id*. at 13.)

For the gross negligence claim, the reply highlights that the alleged vulnerability was publicly discussed on a forum, and Cloudflare responded and fixed the issue within two days, which it argues is inconsistent with recklessness. (*Id*. at 14.) It also contends that Celsius' allegation of a failure to guard against a risk does not amount to the extreme or outrageous conduct necessary to sustain a gross negligence claim. (*Id*.)

II. LEGAL STANDARD

To survive a motion to dismiss brought under Rule 12(b)(6), made applicable here by FED. R. BANK. P. 7012, "a complaint must contain sufficient factual matter . . . to 'state a claim to relief that is plausible on its face.' " *Ashcroft v. Iqbal,* 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly,* 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (citing *Twombly,* 550 U.S. at 556). "While a complaint attacked by a Rule 12(b)(6) motion to dismiss does not need detailed factual allegations, a plaintiff's obligation to provide the grounds of his entitlement to relief requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Twombly,* 550 U.S. at 555 (internal quotation marks, citations, and alterations omitted). Thus, unless a plaintiff's well-pleaded allegations have "nudged [its] claims across the line from conceivable to plausible, [the plaintiff's] complaint must be dismissed." *Id.* at 570; *see also Iqbal,* 556 U.S. at 679.

Courts use a two-prong approach when considering a motion to dismiss. *McHale v. Citibank, N.A. (In re the 1031 Tax Group, LLC),* 420 B.R. 178, 189–90 (Bankr. S.D.N.Y. 2009). First, the court must accept all factual allegations in the complaint as true, discounting legal conclusions clothed in factual garb. *See, e.g., Kiobel v. Royal Dutch Petroleum Co.,* 621 F.3d

111, 124 (2d Cir.2010) (stating that a court must "assum[e] all well-pleaded, nonconclusory factual allegations in the complaint to be true") (citing *Iqbal,* 556 U.S. at 678–79). Second, the court must determine if these well-pleaded factual allegations state a "plausible claim for relief." *Iqbal,* 556 U.S. at 679 (citation omitted).

Courts do not make plausibility determinations in a vacuum; it is a "context specific task that requires the reviewing court to draw on its judicial experience and common sense." *Id.* (citation omitted). A claim is plausible when the factual allegations permit "the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* at 678 (citation omitted). A complaint that only pleads facts that are "merely consistent with a defendant's liability" does not meet the plausibility requirement. *Id.* (quoting *Bell Atl. Corp. v. Twombly,* 550 U.S. at 557) (internal quotation marks omitted). "A pleading that offers 'labels and conclusions' or a 'a formulaic recitation of the elements of a cause of action will not do.'" *Id.* (quoting *Twombly,* 550 U.S. at 555) (internal quotation marks omitted). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id.* (citation omitted). "The pleadings must create the possibility of a right to relief that is more than speculative." *Id.*; *In re MF Glob. Holdings Ltd*, No. 11-15058 (MG), 2013 WL 4511863, at *3 (Bankr. S.D.N.Y. Aug. 23, 2013), *rev'd sub nom*. *In re MF Glob. Holdings, Ltd.*, No. 13 CIV. 07218 LGS, 2014 WL 4054281 (S.D.N.Y. Aug. 14, 2014)

III. DISCUSSION

A. Negligence Claim

To show negligence under New York law, a plaintiff must demonstrate (1) the defendant owed the plaintiff a cognizable duty of care; (2) the defendant breached that duty; and (3) the plaintiff suffered damage as a proximate result. *Ferreira v. City of Binghamton*, 975 F.3d 255,

266 (2d Cir. 2020) (quoting *Williams v. Utica Coll. of Syracuse Univ.*, 453 F.3d 112, 116 (2d Cir. 2006)).

1. Duty

New York courts have recognized that a duty could be predicated on the danger of third-party misconduct where a relationship between the defendant and either the plaintiff or the third-party wrongdoer provides the defendant with the ability to minimize the risk. *Hamilton v. Accu-Tek*, 62 F. Supp. 2d 802 (E.D.N.Y. 1999), *vacated sub nom*. *Hamilton v. Beretta U.S.A. Corp.*, 264 F.3d 21 (2d Cir. 2001). Examples include the relationship between a carrier and its passenger or a tavern owner and its patron, where the defendant is obligated to take reasonable steps to protect from foreseeable risks, including the criminal conduct of others. (*Id*.) "The injured party must show that a defendant owed not merely a general duty to society but a specific duty to him or her, for without a duty running directly to the injured person there can be no liability in damages, however careless the conduct or foreseeable the harm. That is required in order to avoid subjecting an actor to limitless liability to an indeterminate class of persons conceivably injured by any negligence in that act." *Hamilton v. Beretta U.S.A. Corp.*, 96 N.Y.2d 222, 232, 727 N.Y.S.2d 7, 750 N.E.2d 1055 (2001) (first quoting *Lauer*, 95 N.Y.2d at 96, 711 N.Y.S.2d 112, 733 N.E.2d 184; and then quoting *Eiseman v. State*, 70 N.Y.2d 175, 188, 518 N.Y.S.2d 608, 511 N.E.2d 1128 (1987)); *Toretto v. Donnelley Fin. Sols., Inc.*, 583 F. Supp. 3d 570, 593 (S.D.N.Y. 2022).

Courts have extended this principle to cybersecurity contexts. In *Toretto*, 583 F. Supp. 3d 570, the court held that a proxy services provider owed a duty to reasonably safeguard plaintiffs' personal information. The court noted that defendant was in the best position to protect the information on its servers, understood the importance of data security, knew it was a

target of cyber-attacks, and promoted its data security measures to customers. The court emphasized that imposing a duty would not result in limitless liability, as it would be limited to individuals whose information the defendant obtained while providing its service. Similarly, in *Koeller v. Numrich Gun Parts Corp.*, 675 F. Supp. 3d 260 (N.D.N.Y. 2023), the court found that the plaintiffs plausibly alleged a breach of duty by the defendant in failing to exercise reasonable care in securing and handling personal information, supervising agents, and timely notifying customers of a data breach. These cases support the conclusion that where a defendant undertakes to provide cybersecurity-related services and is in a unique position to prevent foreseeable harm to a limited party, a duty may arise under New York law.

Here, Celsius alleges that Cloudflare undertook responsibility for securing access to API keys for the BadgerDAO platform and for warning users of known vulnerabilities. Cloudflare's failure to address or disclose the flaw could create a foreseeable risk of harm to Celsius who used BadgerDAO platform to store substantial digital assets. Accordingly, Celsius has plausibly alleged that Cloudflare owed it a duty of care.

2. Breach

In the Complaint, Celsius alleges that Cloudflare failed to implement and enforce appropriate verification protocols before issuing API keys and failed to notify users once it discovered the vulnerability in its system. Celsius alleged that the failure to implement standard account verification procedures and to provide timely notice of a known vulnerability deviates from both industry practices and the care expected of a reasonably prudent service provider handling sensitive authentication infrastructure.

These allegations are sufficient to plausibly allege that Cloudflare breached its duty. *See In re GE/CBPS*, 2021 WL 3406374, at *8 (finding allegations sufficient to sustain a negligence

claim where the complaint alleged that defendants failed to adopt and oversee appropriate data security processes and hardware systems to safeguard and protect the personal and financial information entrusted to them, despite a reasonably foreseeable risk of unauthorized disclosure); *Sackin*, 278 F. Supp. 3d at 748 (finding allegations sufficient to sustain a negligence claim where the complaint alleged that the defendant was aware of the sensitivity of personal data but failed to take reasonable steps to prevent the wrongful dissemination including erecting a digital firewall, conducting data security training and adopting retention and destruction policies); *see also Toretto*, 583 F. Supp. 3d 570 (S.D.N.Y. 2022) (finding allegations sufficient to sustain a negligence claim where the complaint alleged the defendant was aware of ongoing cyber threats but failed to safeguard personal information it collected and maintained).

3. Damages

Celsius has sufficiently alleged that it suffered damages as a proximate result of Cloudflare's alleged negligence. Specifically, Celsius claims that due to Cloudflare's failure to implement adequate verification protocols and to warn of a known vulnerability, a hacker was able to exploit an unverified API key, gain unauthorized access to the BadgerDAO platform, and execute fraudulent fund transfers. As a result, Celsius allegedly lost over $50 million in digital assets stored on the platform.

At the pleading stage, these allegations are adequate to plausibly support the element of damages. Courts have found such actual economic harm sufficient to satisfy the damages element of a negligence claim. *See Toretto*, 583 F. Supp. 3d 570; *In re GE/CBPS*, 2021 WL 3406374, at *9.

Cloudflare argues that Celsius' allegations on causation are "reed-thin," and that certain actions by BadgerDAO, third-party hackers, or Celsius are intervening causes to Cloudflare's

breach. While other actors may have played a role, proximate cause under New York law does not require that the defendant's negligence be the sole cause of harm—only that it be a substantial factor. *See In re Methyl Tertiary Butyl Ether (MTBE) Prods. Liab. Litig.*, 739 F. Supp. 2d 576, 596 (S.D.N.Y. 2010). Intervening acts do not sever the causal chain where the risk of such acts was foreseeable. Accordingly, Celsius has plausibly alleged that Cloudflare's negligence was a proximate cause of its injury.

Accordingly, Cloudflare's motion to dismiss the negligence claim is **DENIED**.

B. Gross Negligence Claim

Under New York law, "to prevail on a claim for gross negligence, plaintiff must establish" the elements necessary to prevail on a claim for negligence—(1) duty; (2) breach; and (3) injury—plus a fourth element, namely, that defendant's conduct "evinces a reckless disregard for the rights of others or 'smacks' of intentional wrongdoing." *Farash v. Cont'l Airlines, Inc.*, 574 F. Supp. 2d 356, 367–68 (S.D.N.Y. 2008), *aff'd*, 337 F. App'x 7 (2d Cir. 2009) (quoting *AT&T v. City of New York*, 83 F.3d 549, 556 (2d Cir. 1996)). To constitute gross negligence, the act or omission must be of an aggravated character, as distinguished from the failure to exercise ordinary care. *Am. Auto. Ins. Co. v. Rest Assured Alarm Sys., Inc.*, 786 F. Supp. 2d 798, 807 (S.D.N.Y. 2011) (citation omitted).

New York courts have analyzed whether conduct is sufficiently aggravated to constitute gross negligence in an analogous context: the provision and maintenance of fire and burglar alarm services. "Generally, no issue of gross negligence is raised where the claim is based upon either inappropriate installation of an alarm system or an inappropriate response to an alarm. . . . On the other hand, a sufficient issue regarding gross negligence has been held to have been raised in cases referred to as including 'outrageous acts of folly.'" *Metro. Prop. & Cas. Ins. Co.*

v. Budd Morgan Cent. Station Alarm Co., 95 F. Supp. 2d 118, 122–23 (E.D.N.Y. 2000) (citation omitted). Thus, for example, the New York Court of Appeals has found that a plaintiff "alleged much more than mere failure to install a proper working alarm system and inspect it," because the plaintiff alleged that "defendants had knowledge—for weeks, if not months—that the equipment had been malfunctioning" and "that defendants not only failed to investigate the source of their equipment malfunction, but they failed to put anyone at the branch on notice of the potential security breach." *Abacus Fed. Sav. Bank v. ADT Sec. Servs., Inc.*, 18 N.Y.3d 675, 944 N.Y.S.2d 443, 967 N.E.2d 666, 669 (2012). Similarly, the First Department has found that a jury could find that an alarm company was grossly negligent when it failed to send guards to a jewelry manufacturer eleven hours after a weekend break-in and the manufacturer had not alerted the alarm company that it would be open over the weekend. *Rand & Paseka Mfg. Co. v. Holmes Prot. Inc.*, 130 A.D.2d 429, 515 N.Y.S.2d 468, 469–70 (1st Dep't 1987); *see also Hanover Ins. Co. v. D & W Cent. Station Alarm Co.*, 164 A.D.2d 112, 560 N.Y.S.2d 293, 295–96 (1st Dep't 1990) (finding summary judgment for alarm company inappropriate where the record indicated that the alarm company received three signals over four hours, did not notify the police, and directed the guard sent to investigate the issue to "forget the assignment" when he encountered difficulty entering the building). But courts have found insufficient to find gross negligence "failure to wire a skylight," which burglars broke through to steal paintings, *Colnaghi, U.S.A., Ltd. v. Jewelers Prot. Servs., Ltd.*, 81 N.Y.2d 821, 595 N.Y.S.2d 381, 611 N.E.2d 282, 284 (1993), or "an alarm company's delayed or inadequate response to an alarm signal, without more," *Abacus Fed. Sav. Bank v. ADT Sec. Servs., Inc.*, 77 A.D.3d 431, 908 N.Y.S.2d 654, 656 (1st Dep't 2010), *aff'd as modified*, 18 N.Y.3d 675, 944 N.Y.S.2d 443, 967 N.E.2d 666 (2012) (collecting cases); *Am. Auto. Ins. Co.*, 786 F. Supp. 2d 807. In *Yuille v.*

Uphold HQ Inc., 686 F. Supp. 3d 323 (S.D.N.Y. 2023), the court found that the plaintiff sufficiently alleged gross negligence where the defendant was aware of increased hacking activity, was explicitly warned about a potential security breach, and failed to act for over two days while unauthorized transactions occurred.

In this case, Celsius alleges that Cloudflare, a leading cybersecurity service provider, was repeatedly warned about a critical vulnerability in its API key system that permitted unauthorized access to platforms like BadgerDAO, yet it failed to take corrective action or notify users—including Celsius—for an extended period. This alleged failure occurred in the context of heightened risk, where Cloudflare knew or should have known that the compromised API keys could grant access to platforms securing millions in digital assets. Much like the defendant in *Yuille*, who was explicitly warned of a breach and failed to act for over two days during which unauthorized activity occurred, Cloudflare is alleged to have ignored repeated warnings over a longer period and failed to implement even minimal protective measures. Moreover, the Complaint asserts that Cloudflare did not issue any notification to users after discovering the vulnerability, allowing the unauthorized access to continue undetected. Taken together, these facts plausibly support an inference of reckless disregard rather than mere carelessness, and supporting denial of the motion to dismiss the gross negligence claim at this stage.

Accordingly, the Cloudflare's motion to dismiss the gross negligence claim is **DENIED**.

IV. CONLUSION

For the reasons explained above, Cloudflare's Motion is **DENIED.**

IT IS SO ORDERED.

Dated: May 6, 2025
New York, New York

Martin Glenn

MARTIN GLENN
Chief United States Bankruptcy Judge